What is claimed is:

1. A method of protecting a victim site against a denial of service attack, the method comprises:

receiving network packets with faked source addresses;

receiving from the victim site a notification that the victim site is under an attack; and

sending queries to data collectors to request information from at least some of the data collectors, the information to determine the source of suspicious network traffic being sent to the victim.

2. The method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for information based on victim destination address.

3. The method of claim 1 wherein based on collected information the method further comprises:

determining what data centers are performing the spoofing on the victim.

4. The method of claim 3 wherein determining is performed by a control center, and determining further comprising:

sending data to/from a gateway device that is associated with the victim center.

5. The method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center.

6. The method of claim 5 wherein the message is sent over a hardened network.

7. The method of claim 5 wherein message indicates the type of attack.

8. The method of claim 1 wherein the attacker is behind a gateway.

9. The method of claim 8 wherein if the attacker is behind a gateway, the control center issues a request to the gateway that the attacker is behind to block the attacking traffic.

10. The method of claim 8 wherein if the attacker is behind a gateway, the gateway that the attacker is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

11. The method of claim 1 wherein if the attacker is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attackers.

12. The method of claim 1 wherein if the attacker is not behind a gateway, the method further comprises:

contacting administrators at locations involved in attack to have the administrators take action to filter out packets with the destination address.

13. The method of claim 1 wherein the attack is a low-grade spoofing-type of attack that does not compromise

network traffic flow between the victim data center and Internet.

14. The method of claim 1 wherein the attack is a high-grade attack that compromises network traffic flow between the victim data center and Internet.

15. A method of protecting a victim site against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses;

receiving a notification that the victim data center is under an attack, from a gateway disposed near the victim site;

sending queries to data collectors to request information from data collectors that have examined network traffic with the victim destination address; and

determining the data center or centers involved in the attack on the victim by analyzing collected information from the data collectors.

16. The method of claim 15 wherein the control center also includes a communication process to send data to/from a gateway device that is disposed with the victim center.

17. The method of claim 16 wherein if the attacker is behind a gateway, the control center issues a request to the gateway to block the attacking traffic.

18. The method of claim 17 wherein if the attacker is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

19. The method of claim 15 wherein if the attacker is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address.

20. A system to thwart denial of service attacks on a victim, comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic;

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack; and

send queries to data collectors to request information from data collectors, the information used to determine the source of suspicious network traffic being sent to the victim;

a gateway device that passes network packets between the network and the victim site, the gateway disposed to protect the victim site, and being coupled to the control center.